IN THE SPECIFICATION

Please replace the paragraph at page 1, lines 6-12, with the following rewritten paragraph:

The present invention relates to an information processing apparatus, an information processing method, and a program storage medium, and more particularly, to an information processing apparatus, an information processing method, and a program storage medium, which make it possible to prevent data from being ~~tempered~~ tampered or copied in an unauthorized manner.

Please replace the paragraph at page 3, lines 16-24, with the following rewritten paragraph:

8. The various functions described above are realized on a personal computer by means of software. Therefore, if the software is ~~tempered~~ tampered, it may become possible to operate the computer in a manner different from that intended by a system designer.

In view of the above, an object of the present invention is to provide a technique for preventing content data stored on a hard disk from being ~~tempered~~ tampered or copied in an unauthorized manner.

Please replace the paragraph at page 12, lines 10-22, with the following rewritten paragraph:

If a WWW (World Wide ~~Ueb~~ Web) server 5-1 receives a request from the personal computer 1, the WWW server 5-1 transmits data representing information (as to for example the album title and the manufacturer of the CD)associated with the CD a content of which is read and data representing information (as to for example the content title and the composer name) associated with the content to the personal computer 1 via the network 2. If a WWW

(World Wide ~~Ueb~~ Web) server 5-2 receives a request from the personal computer 1, the WWW server 5-2 transmits data representing information associated with the CD a content of which is read and data representing information associated with the content to the personal computer 1 via the network 2.

Please replace the paragraph at page 29, line 16-page 30, line 2, with the following rewritten paragraph:

Before copying, moving, checking-in, or checking-out a content, the usage rule management program 140 checks whether the usage rule data has been ~~tempered~~ tampered, on the basis of the hash value (which will be described later) corresponding to the usage rule data described in the usage rule files 162-1 to 162-N stored in the content database 114. If usage rule data described in any of the usage rule files 162-1 to 162-N stored in the content database 114 is updated in response to the operation of copying, moving, checking-in or checking-out a content, the usage rule management program 140 updates the hash value corresponding to the updated usage rule data.

Please replace the paragraph at page 37, lines 1-20, with the following rewritten paragraph:

A content file stored in the flash memory 61 of the portable device 6 includes a header portion and a data portion, as shown in Fig. 5. In the header portion, information as to the content identifier, the number of reproducing operations, the reproduction limit, the content title, and the artist name is described. On the other hand, in the data portion, a content compressed according to a compression method such as ATRAC-3 and encrypted is described. In order to prevent the content from being ~~tempered~~ tampered, an MAC (message authentication code) value is described in the header portion of the content file. The MAC

value is calculated using a unidirectional function (such as SHA or DES) called a keyed hash in accordance with equation (1) shown below:

MAC Value = MAC(Kc, Important Information) (1)

where Kc is the content key (encryption key) used to encrypt the content described in the data portion, and Important Information is particular part (as to, for example, the content identifier, the number of reproducing operations performed, and the reproduction limit) of the information described in the header portion.

Please replace the paragraph at page 40, line 18-page 41, line 9, with the following rewritten paragraph:

In step S2, the user condition management program 140 calculates the MAC value from the encryption key Kc and the important information described in the header portion of the content file obtained in step S1, in accordance with equation (1) described above. The resultant value is substituted into R. In step S3, the usage rule management program 140 compares the value of R calculated in step S2 with the previous MAC value described in the header portion of the content file. If these two values are not equal to each other, the usage rule management program 140 goes to step S4. In step S4, the display control program displays a message such as "There is a possibility that the content may have [[be]] <u>been</u> ~~tempered~~ <u>tampered</u>." on the display 20, and the process is terminated. In this case, the content stored in the flash memory 61 of the portable device 6 is regarded as being tampered, and thus it is not reproduced.